

FAST COMPUTATION OF THE NUMBER OF SOLUTIONS TO

$$x_1^2 + \cdots + x_k^2 \equiv \lambda \pmod{n}$$

JOSÉ MARÍA GRAU AND ANTONIO M. OLLER-MARCÉN

ABSTRACT. In this paper we study the multiplicative function $\rho_{k,\lambda}(n)$ that counts the number of incongruent solutions of the equation $x_1^2 + \cdots + x_k^2 \equiv \lambda \pmod{n}$. In particular we give closed explicit formulas for $\rho_{k,\lambda}(p^s)$ with a arithmetic complexity of constant order.

1. INTRODUCTION

Let k , λ and n be positive integers and let $\rho_{k,\lambda}(n)$ denote the number of incongruent solutions of the equation

$$x_1^2 + x_2^2 + \cdots + x_k^2 \equiv \lambda \pmod{n}.$$

In other terms:

$$\rho_{k,\lambda}(n) := \text{card} \{ (x_1, \dots, x_k) \in (\mathbb{Z}/n\mathbb{Z})^k : x_1^2 + \cdots + x_k^2 \equiv \lambda \pmod{n} \}$$

Since the function $\rho_{k,\lambda}$ is multiplicative, it is enough to consider the case when $n = p^s$ is a prime power. Moreover, it is also clear that we can introduce the restriction $0 \leq \lambda < n$.

The computation of $\rho_{k,\lambda}(n)$ by mere exhaustive search is obviously inefficient since its computational complexity has order $\Theta(n^k)$. Thus, the interest to find closed formulas involving a number of operations which is as small as possible.

Identities for $\rho_{k,\lambda}(n)$ can be derived using Gauss and Jacobi sums. In fact, we have (see [7]) a very compact expression like:

$$(1) \quad \rho_{k,\lambda}(n) = \frac{1}{n} \sum_{a=1}^n e^{-2\pi i \frac{a\lambda}{n}} \left(\sum_{x=1}^n e^{2\pi i \frac{ax^2}{n}} \right)^k.$$

This expression has theoretical value and it could even be practically applied for small values of n . Nevertheless, it is not useful for moderately big values of n , even in the particularly simple case $\lambda = 0$. This is because the arithmetic complexity of that formula is $\Theta(n^2)$.

Another compact expression can be found in [5]. Namely,

$$(2) \quad \rho_{k,\lambda}(n) = n^{k-1} \sum_{d|n} \frac{1}{d^k} \sum_{\substack{l=1 \\ \gcd(l,r)=1}}^d e^{-\frac{2\pi i l \lambda}{d}} S(l, d)^k,$$

1

where $S(l, r)$ is the quadratic Gauss sum defined by

$$S(l, r) := \sum_{\substack{j=1 \\ \gcd(l, r)=1}}^r \exp(2\pi i l j^2 / r).$$

This formula is also inefficient, even in the prime-power case. In fact, if $n = p^s$ the arithmetic complexity is $\Theta(s^3)$.

Some efficient explicit formulas are known for some particular cases. For instance, V.H. Lebesgue [2] gave in 1837 a closed formula for $\rho_{k,\lambda}(p)$. In [3, p. 46] a formula for $\rho_{k,0}(p^s)$ is given and the case $\gcd(\lambda, p) = 1$ was completely solved in [4] giving. Finally, in [5] and [6] we can find closed formulas for some particular cases of k and λ .

Nevertheless, up to date, no general formula with constant (independent of k , λ and s) complexity for the computation of $\rho_{k,\lambda}(p^s)$ has been given. Thus, with the results that are known today it is not possible to compute (in a reasonable time) the value of $\rho_{10,5^{100000}}(5^{1000000})$, for instance.

In this work, we present explicit general formulas for $\rho_{k,\lambda}(p^s)$ with arithmetic complexity of constant order, $O(1)$. We use elementary techniques that do not involve Gauss or Jacobi sums.

2. KNOWN BASIC CASES

The formulas for $\rho_{k,\lambda}(p^s)$ that we are going to present ultimately rely on the values of $\rho_{k,\lambda}(p)$ if p is an odd prime and on the values of $\rho_{k,\lambda}(2^s)$ with $1 \leq s \leq 3$ if $p = 2$.

As we already pointed out, when p is an odd prime the values of $\rho_{k,\lambda}(p)$ were already studied by V.H. Lebesgue in 1837. In particular he proved the following result [2, Chapter X], where $\left(\frac{\lambda}{p}\right)$ denotes the Legendre symbol defined by

$$\left(\frac{\lambda}{p}\right) = \begin{cases} 1, & \text{if } \lambda \text{ is a quadratic residue modulo } p; \\ -1, & \text{if } \lambda \text{ is not a quadratic residue modulo } p; \\ 0, & \text{if } p \mid \lambda. \end{cases}$$

Proposition 1. *Let p be an odd prime and let k, λ be positive integers with $0 \leq \lambda < p$. Put $t = (-1)^{(p-1)(k-1)/4} p^{(k-1)/2}$ and $l = (-1)^{k(p-1)/4} p^{(k-2)/2}$. Then,*

$$\rho_{k,\lambda}(p) = \begin{cases} p^{k-1} + \left(\frac{\lambda}{p}\right) t, & \text{If } k \text{ is odd;} \\ p^{k-1} - l + \left(1 - \left|\left(\frac{\lambda}{p}\right)\right|\right) pl, & \text{If } k \text{ is even.} \end{cases}$$

In the $p = 2$ case, formulas for $\rho_{k,\lambda}(2^s)$ with $1 \leq s \leq 3$ were given in [4] when λ is even. Here we complete it.

Proposition 2. *Let k be a positive integer. Then:*

- i) $\rho_{k,1}(2) = \rho_{k,0}(2) = 2^{k-1}$,
- ii) $\rho_{k,0}(4) = 4^{-1+k} + 2^{-1+\frac{3k}{2}} \cos(\frac{k\pi}{4})$,
- iii) $\rho_{k,1}(4) = 4^{k-1} + 2^{\frac{3k}{2}-1} \sin(\frac{\pi k}{4})$,
- iv) $\rho_{k,2}(4) = 4^{-1+k} - 2^{-1+\frac{3k}{2}} \cos(\frac{k\pi}{4})$,
- v) $\rho_{k,3}(4) = 4^{k-1} - 2^{\frac{3k}{2}-1} \sin(\frac{\pi k}{4})$,
- vi) $\rho_{k,0}(8) = 8^{-1+k} + 2^{-2+2k} \cos(\frac{k\pi}{4}) + 2^{-2+\frac{5k}{2}} \cos(\frac{k\pi}{4}) + 2^{-2+2k} \cos(\frac{3k\pi}{4})$

$$\begin{aligned}
\text{vii)} \quad \rho_{k,1}(8) &= 2^{2k-3} \left(2^k + 2^{\frac{k}{2}+1} \sin\left(\frac{\pi k}{4}\right) + 2 \sin\left(\frac{1}{4}\pi(k+1)\right) - 2 \cos\left(\frac{1}{4}(3\pi k + \pi)\right) \right), \\
\text{viii)} \quad \rho_{k,2}(8) &= 8^{-1+k} - 2^{-2+\frac{5k}{2}} \cos\left(\frac{k\pi}{4}\right) + 2^{-2+2k} \sin\left(\frac{k\pi}{4}\right) - 2^{-2+2k} \sin\left(\frac{3k\pi}{4}\right) \\
\text{ix)} \quad \rho_{k,3}(8) &= 2^{2k-3} \left(2^k - 2^{\frac{k}{2}+1} \sin\left(\frac{\pi k}{4}\right) - 2 \left(\cos\left(\frac{1}{4}\pi(k+1)\right) + \cos\left(\frac{3}{4}\pi(k+1)\right) \right) \right), \\
\text{x)} \quad \rho_{k,4}(8) &= 8^{-1+k} - 2^{-2+2k} \cos\left(\frac{k\pi}{4}\right) + 2^{-2+\frac{5k}{2}} \cos\left(\frac{k\pi}{4}\right) - 2^{-2+2k} \cos\left(\frac{3k\pi}{4}\right) \\
\text{xi)} \quad \rho_{k,5}(8) &= 2^{2k-3} \left(2^k + 2^{\frac{k}{2}+1} \sin\left(\frac{\pi k}{4}\right) - 2 \sin\left(\frac{1}{4}\pi(k+1)\right) + 2 \cos\left(\frac{1}{4}(3\pi k + \pi)\right) \right), \\
\text{xii)} \quad \rho_{k,6}(8) &= 8^{-1+k} - 2^{-2+\frac{5k}{2}} \cos\left(\frac{k\pi}{4}\right) - 2^{-2+2k} \sin\left(\frac{k\pi}{4}\right) + 2^{-2+2k} \sin\left(\frac{3k\pi}{4}\right), \\
\text{xiii)} \quad \rho_{k,7}(8) &= 2^{2k-3} \left(2^k - 2^{\frac{k}{2}+1} \sin\left(\frac{\pi k}{4}\right) - 2 \sin\left(\frac{1}{4}(3\pi k + \pi)\right) + 2 \cos\left(\frac{1}{4}\pi(k+1)\right) \right).
\end{aligned}$$

Proof. Given $k, n \in \mathbb{N}$, let us define the matrix $M(n) = (\rho_{1,i-j}(n))_{0 \leq i, j \leq n-1}$. If we consider the column vector $R_k(n) = (\rho_{k,i}(n))_{0 \leq i \leq n-1}$, the following recurrence relation holds:

$$R_k(n) = M(n) \cdot R_{k-1}(n).$$

Then, it is enough to apply elementary linear algebra techniques. For details, see [4, Lemma 4]. \square

3. PREPARATORY RESULTS

Given positive integers k, n and $0 \leq \lambda < n$, let $A(k, \lambda, n)$ denote the set of solutions $(x_1, \dots, x_k) \in (\mathbb{Z}/n\mathbb{Z})^k$ of the congruence $x_1^2 + \dots + x_k^2 \equiv \lambda \pmod{n}$. In particular, if $n = p^s$ is a prime-power, we have that

$$A(k, \lambda, p^s) = \{(x_1, \dots, x_k) \in (\mathbb{Z}_{p^s})^k : x_1^2 + \dots + x_k^2 \equiv \lambda \pmod{p^s}\}.$$

Now, in this situation, let us define the following sets:

$$A_1(k, \lambda, p^s) = \{(x_1, \dots, x_k) \in A(k, \lambda, p^s) : p \nmid x_i \text{ for some } 1 \leq i \leq k\},$$

$$A_2(k, \lambda, p^s) = \{(x_1, \dots, x_k) \in A(k, \lambda, p^s) : p \mid x_i \text{ for every } 1 \leq i \leq k\}.$$

Note that $A(k, \lambda, p^s) = A_1(k, \lambda, p^s) \cup A_2(k, \lambda, p^s)$. Hence, since $A_1(k, \lambda, p^s)$ and $A_2(k, \lambda, p^s)$ are disjoint, if we define $\rho_{k,\lambda}^{(1)}(p^s) := \text{card}(A_1(k, \lambda, p^s))$ and $\rho_{k,\lambda}^{(2)}(p^s) := \text{card}(A_2(k, \lambda, p^s))$ it follows that

$$\rho_{k,\lambda}(p^s) = \rho_{k,\lambda}^{(1)}(p^s) + \rho_{k,\lambda}^{(2)}(p^s).$$

Remark 1. If $\gcd(\lambda, p) = 1$; i.e., if $p \nmid \lambda$ then $A_2(k, \lambda, p^s) = \emptyset$. Thus, $\rho_{k,\lambda}^{(2)}(p^s) = 0$ and it follows that $\rho_{k,\lambda}^{(1)}(p^s) = \rho_{k,\lambda}(p^s)$.

This remark implies that the proof of the following result is the same as that of Lemmata 1 and 2 in [4].

Proposition 3.

i) Let p^s be an odd prime-power with $s \geq 1$ and $0 \leq \lambda < p^s$. Then,

$$\rho_{k,\lambda}^{(1)}(p^s) = p^{(s-1)(k-1)} \rho_{k,\lambda}^{(1)}(p).$$

ii) Let $s \geq 3$ and $0 \leq \lambda < 2^s$. Then, $\rho_{k,\lambda}^{(1)}(2^s) = 2^{(s-3)(k-1)} \rho_{k,\lambda}^{(1)}(8)$.

Proposition 3 provides us with a recursive relation for $\rho_{k,\lambda}^{(1)}(p^s)$. Note that this result implies that we will have to study the case $p = 2$ separately.

Now we turn to $\rho_{k,\lambda}^{(2)}(p^s)$. In this case, we have the following result.

Proposition 4. *Let p^s be a prime-power, with $s \geq 1$ and let $0 \leq \lambda < p^s$. Then,*

$$\rho_{k,\lambda}^{(2)}(p^s) = \begin{cases} 1, & \text{if } s = 1 \text{ and } \lambda = 0; \\ p^k, & \text{if } s = 2 \text{ and } \lambda = 0; \\ p^k \rho_{k,\lambda/p^2}(p^{s-2}), & \text{if } s \geq 3 \text{ and } p^2 \mid \lambda; \\ 0, & \text{otherwise.} \end{cases}$$

Proof. If $s = 1$ and $\lambda = 0$, it is obvious that the only k -tuple (x_1, \dots, x_k) such that $x_1^2 + \dots + x_k^2 \equiv 0 \pmod{p}$ and $p \mid x_i$ for every i is $(0, \dots, 0)$. Hence, $\rho_{k,\lambda}^{(2)}(p^s) = 1$ in this case.

Secondly, if $s = 2$ and $\lambda = 0$, $\rho_{k,\lambda}^{(2)}(p^2) = \rho_{k,0}^{(2)}(p^2)$ is the number of k -tuples (x_1, \dots, x_k) such that $x_1^2 + \dots + x_k^2 \equiv 0 \pmod{p^2}$ and $p \mid x_i$ for every i . It is obvious that there are p^k such k -tuples because x_i can be any multiple of p in $\mathbb{Z}/p^2\mathbb{Z}$.

Now, assume that $p^2 \mid \lambda$ and $s \geq 3$. First of all, using Euclid's algorithm, it is easy to see that every element of $A_2(k, \lambda, p^s)$ can be written in the form $(px_1 + \alpha_1 p^{s-1}, \dots, px_k + \alpha_k p^{s-1})$ with $0 \leq \alpha_i \leq p-1$ and $(x_1, \dots, x_k) \in A(k, \lambda/p^2, p^{s-2})$.

On the other hand, let $(x_1, \dots, x_k) \in A(k, \lambda/p^2, p^{s-2})$; i.e., $x_1^2 + \dots + x_k^2 \equiv \lambda/p^2 \pmod{p^{s-2}}$. Clearly the set

$$\{(px_1 + \alpha_1 p^{s-1}, \dots, px_k + \alpha_k p^{s-1}) : 0 \leq \alpha_i \leq p-1 \text{ for every } 1 \leq i \leq k\}$$

is contained in $A_2(k, \lambda, p^s)$ because

$$(px_1 + \alpha_1 p^{s-1})^2 + \dots + (px_k + \alpha_k p^{s-1})^2 \equiv p^2(x_1^2 + \dots + x_k^2) \equiv \lambda \pmod{p^s}$$

and all its elements are incongruent modulo p^s . Thus, every element of the set $A(k, \lambda/p^2, p^{s-2})$ gives rise to p^k different elements of $A_2(k, \lambda, p^s)$ and the result follows.

Finally, in the remaining cases (i.e., if $s = 1$ or 2 with $0 < \lambda < p^2$ or if $s \geq 3$ with $p^2 \nmid \lambda$) it is obvious that $A_2(k, \lambda, p^s) = \emptyset$ and hence $\rho_{k,\lambda}^{(2)}(p^s) = 0$, as claimed. \square

With the help of Proposition 3 and Proposition 4 we can give recursive formulas that express the value of $\rho_{k,\lambda}(p^s)$. First, we deal with the odd p and non-zero λ case.

Theorem 1. *Let p^s be an odd prime-power and let $0 < \lambda < p^s$ be an integer. Put $\lambda = p^r \lambda'$ with $0 \leq r < s$ and $p \nmid \lambda'$. Then,*

$$\rho_{k,\lambda}(p^s) = \sum_{i=0}^{\lfloor r/2 \rfloor} p^{ki + (s-2i-1)(k-1)} \cdot \rho_{k,\lambda/p^{2i}}^{(1)}(p).$$

Proof. We have that $\rho_{k,\lambda}(p^s) = \rho_{k,\lambda}^{(1)}(p^s) + \rho_{k,\lambda}^{(2)}(p^s)$. If $r \leq 1$, then Proposition 4 implies that $\rho_{k,\lambda}^{(2)}(p^s) = 0$. Hence, $\rho_{k,\lambda}(p^s) = \rho_{k,\lambda}^{(1)}(p^s) = p^{(s-1)(k-1)} \rho_{k,\lambda}^{(1)}(p)$ due to Proposition 3 and we are done.

Now, if $r \geq 2$ the $s \geq 3$ and Proposition 4 implies that

$$\rho_{k,\lambda}^{(2)}(p^s) = p^k \rho_{k,\lambda/p^2}(p^{s-2}) = p^k \rho_{k,\lambda/p^2}^{(1)}(p^{s-2}) + p^k \rho_{k,\lambda/p^2}^{(2)}(p^{s-2}).$$

Thus, using Proposition 3 again we obtain that

$$\rho_{k,\lambda}(p^s) = p^{(s-1)(k-1)} \rho_{k,\lambda}^{(1)}(p) + p^k p^{(s-3)(k-1)} \rho_{k,\lambda/p^2}^{(1)}(p) + p^k \rho_{k,\lambda/p^2}^{(2)}(p^{s-2}).$$

Since $\lambda/p^2 = p^{r-2} \lambda'$, if $r-2 \leq 1$, then $\rho_{k,\lambda/p^2}^{(2)}(p^{s-2}) = 0$ by Proposition 4 and we are done.

If, on the other hand, $r \geq 4$ then $s - 2 \geq 3$ and Proposition 4 implies that $\rho_{k,\lambda/p^2}^{(2)}(p^{s-2}) = p^k \rho_{k,\lambda/p^4}^{(2)}(p^{s-4})$. Thus, using Proposition 3 again, it follows that

$$\rho_{k,\lambda}(p^s) = \sum_{i=0}^2 \left(p^{ki+(s-2i-1)(k-1)} \rho_{k,\lambda/p^{2i}}^{(1)}(p) \right) + p^{2k} \rho_{k,\lambda/p^4}^{(2)}(p^{s-4}).$$

Clearly this process can be iteratively repeated until we reach the expression

$$\rho_{k,\lambda}(p^s) = \sum_{i=0}^{\lfloor r/2 \rfloor} \left(p^{ki+(s-2i-1)(k-1)} \cdot \rho_{k,\lambda/p^{2i}}^{(1)}(p) \right) + p^{k \lfloor r/2 \rfloor} \rho_{k,\lambda/p^{2 \lfloor r/2 \rfloor}}^{(2)}(p^{s-2 \lfloor r/2 \rfloor})$$

and, since $p^2 \nmid \lambda/p^{2 \lfloor r/2 \rfloor}$ the result follows from Proposition 4. \square

Now, we turn to the $\lambda = 0$ case for an odd prime p .

Theorem 2. *Let p^s be an odd prime-power. Then,*

$$\rho_{k,0}(p^s) = \sum_{i=0}^{\lfloor (s-1)/2 \rfloor} \left(p^{ki+(s-2i-1)(k-1)} \cdot \rho_{k,p^{s-2i}}^{(1)}(p) \right) + p^{\lfloor s/2 \rfloor k}.$$

Proof. First of all, note that $\rho_{k,0}(p^s) = \rho_{k,p^s}(p^s)$. Then we can proceed recursively just like in Theorem 1 because $\rho_{k,p^s}(p^s) = \rho_{k,p^s}^{(1)}(p^s) + \rho_{k,p^s}^{(2)}(p^s)$.

If $s = 1$, then $\rho_{k,p}(p) = \rho_{k,p}^{(1)}(p) + \rho_{k,p}^{(2)}(p) = \rho_{k,p}^{(1)}(p) + 1$ due to Proposition 4.

If $s = 2$, $\rho_{k,p^2}(p^2) = \rho_{k,p^2}^{(1)}(p^2) + \rho_{k,p^2}^{(2)}(p^2) = p^{k-1} \rho_{k,p^2}^{(1)}(p) + p^k$ due to Propositions 3 and 4.

Now, if $s \geq 3$, then Propositions 3 and 4 imply that

$$\rho_{k,p^s}(p^s) = \rho_{k,p^s}^{(1)}(p^s) + \rho_{k,p^s}^{(2)}(p^s) = p^{(s-1)(k-1)} \rho_{k,p^s}(p) + p^k \rho_{k,p^{s-2}}(p^{s-2})$$

If $s - 2 = 1$ or $s - 2 = 2$, then we apply Proposition 4 and the result follows. If, on the other hand, $s - 2 \geq 3$ then

$$\rho_{k,p^s}(p^s) = p^{(s-1)(k-1)} \rho_{k,p^s}(p) + p^k \left(\rho_{k,p^{s-2}}^{(1)}(p^{s-2}) + \rho_{k,p^{s-2}}^{(2)}(p^{s-2}) \right)$$

so applying Propositions 3 and 4 again we get that

$$\rho_{k,p^s}(p^s) = p^{(s-1)(k-1)} \rho_{k,p^s}(p) + p^k p^{(s-3)(k-1)} \rho_{k,p^{s-2}}(p) + p^k \rho_{k,p^{s-4}}(p^{s-4}).$$

To conclude the proof it is enough to observe that the previous process will end after $\lfloor (s-1)/2 \rfloor$ steps and hence after $\lfloor (s-1)/2 \rfloor + 1$ applications of Propositions 3 and 4. \square

Now, for the case $p = 2$ and non-zero λ we have the following result.

Theorem 3. *Let 2^s be a power of two ($s \geq 1$) and let $0 < \lambda < 2^s$ be an integer. Put $\lambda = 2^r \lambda'$ with $0 \leq r < s$ and odd λ' . Then,*

$$\rho_{k,\lambda}(2^s) = \sum_{i=0}^{\lfloor \frac{r}{2} \rfloor - 1} \left(2^{ki+(s-2i-3)(k-1)} \cdot \rho_{k,\lambda/2^{2i}}^{(1)}(8) \right) + 2^{k \lfloor \frac{r}{2} \rfloor} \rho_{k,\lambda/2^{2 \lfloor \frac{r}{2} \rfloor}}^{(1)}(2^{s-2 \lfloor \frac{r}{2} \rfloor}).$$

Proof. The proof goes exactly as in Theorem 1 using Proposition 3 and Proposition 4 repeatedly. Note that, in the cases $r = 0$ and $r = 1$ we consider that if the upper summation limit is -1 , the sum is empty. \square

And finally, the case $p = 2$, and $\lambda = 0$ is given by the following result.

Theorem 4. *Let 2^s be a power of two ($s \geq 1$). Then,*

$$\rho_{k,0}(2^s) = \sum_{i=0}^{\lfloor \frac{s-1}{2} \rfloor - 1} \left(2^{ki} 2^{(s-2i-3)(k-1)} \cdot \rho_{k,2^{s-2i}}^{(1)}(8) \right) + 2^{\lfloor \frac{s-1}{2} \rfloor k} \cdot \rho_{k,0}^{(1)}(2^{s-2\lfloor \frac{s-1}{2} \rfloor}) + 2^{\lfloor \frac{s}{2} \rfloor k}.$$

Proof. The proof goes exactly as in Theorem 2 using Proposition 3 and Proposition 4 repeatedly. Note that, in the cases $s = 1$ and $s = 2$ we consider that if the upper summation limit is -1 , the sum is empty. \square

4. FAST COMPUTATION OF $\rho_{k,\lambda}(p^s)$

With the results that we have proved in the previous section, we have a procedure to compute $\rho_{k,\lambda}(p^s)$ which has arithmetic complexity of order $O(s)$. Nevertheless, as we are going to see in this section, it is possible to obtain formulas requiring a constant number of operations.

To do so, given integer numbers k , p , s and N , we define the function

$$\Omega(k, p, s, N) := \sum_{i=0}^N p^{ki + (s-2i-1)(k-1)}.$$

Since it is essentially a geometric series, the following result is straightforward.

Lemma 1. *Let k , p , s and N be integer numbers. Then,*

$$\Omega(k, p, s, N) = \begin{cases} \frac{-1+p^{1+N}}{-1+p}, & \text{if } k = 1; \\ p^{-1+s}(1+N), & \text{if } k = 2; \\ \frac{p^{(-1+k)(-1+s)}(p^k - p^2(p^{2-k})^N)}{-p^2 + p^k}, & \text{otherwise.} \end{cases}$$

The following result will also be useful in the sequel.

Lemma 2.

i) *Let p be any prime and let $0 \leq \lambda < p$. Then,*

$$\rho_{k,\lambda}^{(1)}(p) = \begin{cases} \rho_{k,\lambda}(p) - 1, & \text{if } \lambda = 0; \\ \rho_{k,\lambda}(p), & \text{if } \lambda \neq 0. \end{cases}$$

ii) *Let $0 \leq \lambda < 4$. Then,*

$$\rho_{k,\lambda}^{(1)}(4) = \begin{cases} \rho_{k,\lambda}(4) - 2^k, & \text{if } \lambda = 0; \\ \rho_{k,\lambda}(4), & \text{if } \lambda \neq 0. \end{cases}$$

iii) *Let $0 \leq \lambda < 8$. Then,*

$$\rho_{k,\lambda}^{(1)}(8) = \begin{cases} \rho_{k,\lambda}(8) - 2^{2k-1}, & \text{if } \lambda = 0, 4; \\ \rho_{k,\lambda}(8), & \text{if } \lambda \neq 0, 4. \end{cases}$$

Proof. Just recall that $\rho_{k,\lambda}^{(1)}(n) = \rho_{k,\lambda}(n) - \rho_{k,\lambda}^{(2)}(n)$ and apply Proposition 4. \square

Corollary 1. *Let p^s be an odd prime-power and let $0 < \lambda < p^s$ be an integer. Put $\lambda = p^r \lambda'$ with $0 \leq r < s$ and $p \nmid \lambda'$. Then,*

$$\rho_{k,\lambda}(p^s) = \begin{cases} \Omega(k, p, s, \frac{r-1}{2}) \cdot (\rho_{k,0}(p) - 1), & \text{if } r \text{ is odd;} \\ \Omega(k, p, s, \frac{r-2}{2}) \cdot (\rho_{k,0}(p) - 1) + p^{k\frac{r}{2} + (s-r-1)(k-1)} \cdot \rho_{k,\lambda'}(p), & \text{if } r \text{ is even.} \end{cases}$$

Proof. Using Lemma 2 the following hold:

- If r is odd, then for every $i \leq \lfloor r/2 \rfloor$ we have that $\rho_{k,\lambda/p^{2i}}^{(1)}(p) = \rho_{k,0}^{(1)}(p) = \rho_{k,0}(p) - 1$.
- On the other hand, if r is even then $\rho_{k,\lambda/p^{2i}}^{(1)}(p) = \rho_{k,0}^{(1)}(p) = \rho_{k,0}(p) - 1$ for every $i < r/2$, while $\rho_{k,\lambda/p^{2i}}^{(1)}(p) = \rho_{k,\lambda'}(p)$ for $i = r/2$.

Hence, from Theorem 1 it follows that

$$\rho_{k,\lambda}(p^s) = \sum_{i=0}^{r/2-1} p^{ki+(s-2i-1)(k-1)} \cdot (\rho_{k,0}(p) - 1) + p^{kr/2+(s-r-1)(k-1)} \cdot \rho_{k,\lambda'}(p)$$

and Lemma 1 concludes the proof. \square

Corollary 2. *Let p^s be an odd prime-power. Then,*

$$\rho_{k,0}(p^s) = \Omega(k, p, s, \lfloor \frac{s-1}{2} \rfloor) \cdot (\rho_{k,0}(p) - 1) + p^{k\lfloor s/2 \rfloor}$$

Proof. First, observe that $s - 2i > 0$ for every $i \leq \lfloor \frac{s-1}{2} \rfloor$. Thus, Lemma 2 implies that $\rho_{k,p^{s-2i}}^{(1)}(p) = \rho_{k,0}(p) - 1$. Consequently, it is enough to apply theorem 2 to get that

$$\rho_{k,0}(p^s) = (\rho_{k,0}(p) - 1) \cdot \sum_{i=0}^{\lfloor (s-1)/2 \rfloor} \left(p^{ki} p^{(s-2i-1)(k-1)} \right) + p^{\lfloor s/2 \rfloor k}$$

and the result follows. \square

Corollary 3. *Let 2^s be a power of two ($s \geq 3$) and let $0 < \lambda < 2^s$ be an integer. Put $\lambda = 2^r \lambda'$ with $0 \leq r < s$ and odd λ' . Then,*

i) *If r is odd and $s - r > 1$,*

$$\rho_{k,\lambda}(2^s) = \frac{\Omega(k, 2, s, \frac{r-3}{2})}{2^{2(k-1)}} \cdot (\rho_{k,0}(8) - 2^{2k-1}) + 2^{k\frac{r-1}{2}+(s-r-2)(k-1)} \rho_{k,\lambda'2}(8).$$

ii) *If r is odd and $s - r = 1$,*

$$\rho_{k,\lambda}(2^s) = \frac{\Omega(k, 2, s, \frac{r-3}{2})}{2^{2(k-1)}} \cdot (\rho_{k,0}(8) - 2^{2k-1}) + 2^{k\frac{r-1}{2}} \rho_{k,2\lambda'}(4).$$

iii) *If r is even and $s - r > 2$,*

$$\begin{aligned} \rho_{k,\lambda}(2^s) &= \frac{1}{2^{2(k-1)}} \Omega(k, 2, s, \frac{r-4}{2}) \cdot (\rho_{k,0}(8) - 2^{2k-1}) + \\ &+ 2^{1+r-s+k(-2-\frac{r}{2}+s)} (\rho_{k,4\lambda'}(8) - 2^{2k-1}) + 2^{k\frac{r}{2}+(s-r-3)(k-1)} \rho_{k,\lambda'}(8). \end{aligned}$$

iv) *If r is even and $s - r = 2$,*

$$\begin{aligned} \rho_{k,\lambda}(2^s) &= \frac{1}{2^{2(k-1)}} \Omega(k, 2, s, \frac{r-4}{2}) \cdot (\rho_{k,0}(8) - 2^{2k-1}) + \\ &+ 2^{1+r-s+k(-2-\frac{r}{2}+s)} (\rho_{k,4\lambda'}(8) - 2^{2k-1}) + 2^{k\frac{r}{2}} \rho_{k,\lambda'}(4). \end{aligned}$$

v) *If r is even and $s - r = 1$,*

$$\begin{aligned} \rho_{k,\lambda}(2^s) &= \frac{1}{2^{2(k-1)}} \Omega(k, 2, s, \frac{r-4}{2}) \cdot (\rho_{k,0}(8) - 2^{2k-1}) + \\ &+ 2^{1+r-s+k(-2-\frac{r}{2}+s)} (\rho_{k,4\lambda'}(8) - 2^{2k-1}) + 2^{k\frac{r}{2}} \rho_{k,\lambda'}(2). \end{aligned}$$

Proof. i) If r is odd and $s - r > 1$, then $r - 2i \geq 3$ for every $i \leq \lfloor \frac{r}{2} - 1 \rfloor$.
Consequently,

$$\rho_{k,\lambda/2^{2i}}^{(1)}(8) = \rho_{k,0}^{(1)}(8) = \rho_{k,0}(8) - 2^{2k-1}$$

due to Lemma 2 and

$$\sum_{i=0}^{\lfloor \frac{r}{2} \rfloor - 1} \left(2^{ki} 2^{(s-2i-3)(k-1)} \cdot \rho_{k,\lambda/2^{2i}}^{(1)}(8) \right) = \frac{1}{2^{2(k-1)}} \Omega(k, 2, s, r, \frac{r-3}{2}) \cdot (\rho_{k,0}(8) - 2^{2k-1}).$$

Finally, since

$$2^{k \lfloor \frac{r}{2} \rfloor} \rho_{k,\lambda/2^{2 \lfloor \frac{r}{2} \rfloor}}^{(1)}(2^{s-2 \lfloor \frac{r}{2} \rfloor}) = 2^{k \lfloor \frac{r}{2} \rfloor} \rho_{k,2\lambda'}^{(1)}(2^{s-r+1}) = 2^{k \frac{r-1}{2} + (s-r-2)(k-1)} \rho_{k,2\lambda'}(8)$$

the result follows in this case.

ii) If r is odd and $s - r = 1$, we proceed like in the previous case but now we have that

$$2^{k \lfloor \frac{r}{2} \rfloor} \rho_{k,2\lambda'}^{(1)}(2^{s-r+1}) = 2^{k \lfloor \frac{r}{2} \rfloor} \rho_{k,2\lambda'}^{(1)}(4) = 2^{k \lfloor \frac{r}{2} \rfloor} \rho_{k,2\lambda'}(4).$$

iii) If r is even and $s - r > 2$, then $r - 2i \geq 3$ for every $i < \lfloor \frac{r}{2} - 1 \rfloor$, while $r - 2i = 2$ for $i = \lfloor \frac{r}{2} - 1 \rfloor$. Thus,

$$\begin{aligned} & \sum_{i=0}^{\lfloor \frac{r}{2} \rfloor - 1} \left(2^{ki} 2^{(s-2i-3)(k-1)} \cdot \rho_{k,\lambda/2^{2i}}^{(1)}(8) \right) = \\ &= \sum_{i=0}^{\frac{r-4}{2}} \left(2^{ki} 2^{(s-2i-3)(k-1)} \cdot \rho_{k,0}^{(1)}(8) \right) + 2^{1+r-s+k(-2-\frac{r}{2}+s)} (\rho_{k,4\lambda'}^{(1)}(8)) = \\ &= \sum_{i=0}^{\frac{r-4}{2}} \left(2^{ki} 2^{(s-2i-3)(k-1)} \cdot \rho_{k,0}(8) \right) + 2^{1+r-s+k(-2-\frac{r}{2}+s)} (\rho_{k,4\lambda'}(8) - 2^{2k-1}). \end{aligned}$$

iv) and v) If r is even and $1 \leq s - r \leq 2$, we proceed like in the previous case but now we have that

$$2^{k \lfloor \frac{r}{2} \rfloor} \rho_{k,\lambda/2^{2 \lfloor \frac{r}{2} \rfloor}}^{(1)}(2^{s-2 \lfloor \frac{r}{2} \rfloor}) = 2^{k \frac{r}{2}} \rho_{k,\lambda'}^{(1)}(2^{s-r}) = 2^{k \frac{r}{2}} \rho_{k,\lambda'}(2^{s-r}).$$

□

Corollary 4. *Let 2^s be a power of two ($s \geq 3$). Then,*

$$\rho_{k,0}(2^s) = \begin{cases} \frac{1}{2^{2(k-1)}} \Omega(k, 2, s, \frac{s-3}{2}) (\rho_{k,0}(8) - 2^{2k-1}) + 2^{\frac{s-1}{2}k} \cdot 2^{k-1} + 2^{\frac{s-1}{2}}, & \text{if } r \text{ is odd;} \\ \frac{1}{2^{2(k-1)}} \Omega(k, 2, s, \frac{s-4}{2}) (\rho_{k,0}(8) - 2^{2k-1}) + 2^{\frac{s-2}{2}k} \cdot (\rho_{k,0}(4) - 2^k) + 2^{\frac{s}{2}k}, & \text{if } r \text{ is even.} \end{cases}$$

Proof. For every $i \leq \lfloor \frac{s-1}{2} \rfloor - 1$ we have that

$$\rho_{k,2^{s-2i}}^{(1)}(8) = \rho_{k,0}^{(1)}(8) = \rho_{k,0}(8) - 2^{2k-1}.$$

Now, if r is odd

$$\rho_{k,0}^{(1)}(2^{s-2 \lfloor \frac{s-1}{2} \rfloor}) = \rho_{k,0}^{(1)}(2) = 2^{k-1}.$$

While, if r is even

$$\rho_{k,0}^{(1)}(2^{s-2 \lfloor \frac{s-1}{2} \rfloor}) = \rho_{k,0}^{(1)}(4) = \rho_{k,0}(4) - 2^k.$$

In any case, it suffices to apply Theorem 4. □

5. COMPUTATIONAL COMPLEXITY OF THE COMPUTATION OF $\rho_{k,\lambda}(p^s)$

The use of formulas for $\rho_{k,\lambda}(p^s)$ like (1) and (2), based in the use of Gauss sums is ineffective, even for moderate small values of the parameters. For instance, the computation of $\rho_{10,5^{100000}}(5^{1000000})$ using (2) requires more than 10^{18} arithmetic operations. With the formulas that we have presented in this paper, the number of required arithmetic operations is of constant order and the aforementioned value can be computed in a domestic PC almost instantly. However, the mentioned arithmetic operations involve powers of integers as well as the computation of Legendre symbols in order to obtain the value of $\rho_{k,\lambda}(p)$ via Proposition 1. These operations, when considered bit-wise, have a computational cost that increases with the size of the inputs. This becomes apparent when the involved parameters are very big.

If we have a look at the formulas presented in the previous section, those operations whose computational cost dominates over the others are the computation of the power p^{ks} and the computation of the Legendre symbol. Their computational bit-level complexity is, respectively, $O(M(\log(p)) \log(ks))$ and $O(M(\log(p)) \log \log(p))$, where $M(n)$ represents the computational complexity of the chosen multiplication algorithm (see [8]). This gives an idea of which is the influence of each parameter over the overall computational cost of our procedure, as well as of its limitations. In fact, this reveals that the influence of the parameters k and s are similar (logarithmic order complexity) and somewhat lower to that of the prime p when considering, for instance, the Schönhage-Strassen multiplication algorithm whose computational complexity for the product of two numbers of size n is $M(n) = O(n \log(n) \log \log(n))$ (see [9]) or the Fürer's algorithm [10], which runs in time $O(n \log(n) 2^{O(\log^*(n))})$.

REFERENCES

- [1] K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory, 2nd ed., Graduate Texts in Mathematics 84, Springer, 1990.
- [2] Leonard Eugene Dickson. *History of the theory of numbers. Vol. I: Divisibility and primality*. Chelsea Publishing Co., New York, 1966.
- [3] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced
- [4] Calderón, Catalina; Grau, José María; Oller-Marcén Antonio M. and Tóth, László (2015). Counting invertible sums of squares modulo n and a new generalization of euler's totient function. *Publicationes Mathematicae Debrecen* 87 (1-2), pp. 133-145 .
- [5] Tóth, L., Counting Solutions of Quadratic Congruences in Several Variables Revisited, *Journal of Integer Sequences*, 17 (2014), Article 14.11.6.
- [6] C. Calderón, M.J. de Velasco, On divisors of a quadratic form. *Bol Soc Bras. Mat.* , Vol. 31, No 1, 81-91.
- [7] N.M. Korobov, *Las sumas trigonométricas y sus aplicaciones*. Servicio Editorial de la Universidad del País Vasco. 1993.
- [8] Richard P. Brent and Paul Zimmermann, An $O(M(n) \log n)$ algorithm for the Jacobi symbol, *Proc. ANTS-IX*, LNCS 6197 (2010), 83-95.
- [9] A. Schönhage and V. Strassen, Schnelle Multiplikation großer Zahlen , *Computing* 7 (1971), pp. 281-292.
- [10] Fürer, M. (2007). Faster Integer Multiplication. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, June 11-13, 2007, San Diego, California, USA

DEPARTAMENTO DE MATEMÁTICAS, UNIVERSIDAD DE OVIEDO, AVDA. CALVO SOTELLO, s/N, 33007 OVIEDO, SPAIN

E-mail address: grau@uniovi.es

CENTRO UNIVERSITARIO DE LA DEFENSA, CTRA. DE HUESCA, s/N, 50090 ZARAGOZA, SPAIN

E-mail address: oller@unizar.es